IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH ddslogs717@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 21-mj- 271-AJ-01 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, George Jasek, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by Google LLC (Google), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the United States Secret Service and have been so employed since March 5, 2018. I am currently assigned to the Manchester, New Hampshire Resident Office. In preparation for my employment with the United States Secret Service I completed the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement

Training Center in Glynco, Georgia. Additionally, I completed the Special Agent Training Course (SATC) at the United States Secret Service James J. Rowley Training Center in Laurel, Maryland. While attending SATC I received a five-day training titled "Basic Investigation of Computer and Electronic Crimes Program" (BICEP). In addition to these training programs, I have completed numerous in-service training courses related to constitutional law. Prior to my employment with the United States Secret Service, I was a full-time certified Police Officer in Nashua, New Hampshire for over five years. My present duties include the investigation of federal offenses, including, but not limited to, those involving financial fraud and its related activities.

3. As part of my duties I have conducted numerous financial crimes and financial fraud investigations. These investigations have included but are not limited to federal violations of Wire Fraud, Bank Fraud, Money Laundering, and Identity Theft. During the course of these investigations, I have conferred with other investigators who specialize in computer forensics and who have conducted investigations regarding financial fraud crimes. I have additionally received training regarding computers that includes Basic Network Intrusion Responder Training, Incident Response Analysis, and Cryptocurrency training.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (Wire Fraud) have been committed by the user(s) of ddslogs717@gmail.com. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. On July 26, 2021 the Secret Service began investigating a Business Email Compromise (BEC) incident involving the Town of Peterborough, New Hampshire.

8. From my training and experience, I know that a Business Email Compromise (BEC) is a scam/fraud scheme in which bad actors send an email message that appears to come from a known source making a legitimate request. For example, a common type of BEC involves an email that appears to come from a vendor with whom the target company regularly does business. The email requests that the Automated Clearing House (ACH) or wire transfer information for the vendor be changed. Another example is a victim homebuyer that receives a message/email from a title company with instructions on how to wire a down payment. From my training and experience, I know that the emails received from bad actors to the victims of a BEC are typically from a "spoofed" email account or website. A "spoofed email" is an email address with slight variations of a legitimate email address that the victim communicates with (ex: johnsmith@company.com vs. johnsmlth@company.com).

9. From my training and experience, I know an Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent

from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

10. Law enforcement discovered that between on April 7, 2021 and on July 22, 2021, someone using foreign Internet Protocol (IP) addresses started logging into an official email account for Leo Smith, the Finance Director for Peterborough. Smith's email address is @peterboroughnh.gov.

11. The foreign IP address logins to Smith's Peterborough account came from the Netherlands, Ghana, British Virgin Islands, Nigeria, Israel, Peru, Japan, and Brazil.

12. From my training and experience, I know that logins from foreign IP addresses persisting over a period of time from multiple countries indicates that Smith's email credentials were likely compromised and that an unauthorized actor had access to his account.

13. For legitimate business purposes, Leo Smith communicates with Loreal Schmidt, Business Administrator for the Contoocook Valley School District (CONVAL). Schmidt's legitimate email address is @conval.edu.

14. On July 14, 2021 an email was sent to Smith's email account. It was disguised to look like it was coming from Schmidt, when in fact it came from a spoofed email: @convaledu.com. The email contained updated Automated Clearing House (ACH) authorization information for Peterborough's monthly payment to the CONVAL School District. Specifically, the email stated Peterborough should wire funds to Citizens Bank account 639 with ABA Routing/Transit number 50. The email also had an enrollment form and void check attached.

15. On July 23, 2021 Peterborough sent an ACH wire of $1,233,558.59 from the town account with Peoples United (account ending 2298) to the Citizens Bank account ending 8639. The CONVAL School District later advised it never received its monthly payment from Peterborough, triggering this investigation.

16. The Citizens Bank account ending 8639 was opened on March 3, 2021 and is a business account titled "Andrea Perez LLC." The account was opened at the Citizens Bank Greentree Branch located at 980 Route 73 N, Marlton, New Jersey 08053. The listed name on the account is Andrea M Perez, DOB 1980, with an address of Cliffside Park, New Jersey 07010.

17. After the Citizens Bank account titled Andrea Perez LLC (account ending 8639) received the ACH transaction in the amount of $1,233,558.59, someone transferred the funds from that account. As relevant here, on July 23, 2021 $330,100.00 was sent from Citizens Bank ending 8639 to PNC Bank account number 378. The beneficiary information for PNC account ending 0378 was DDS Logistics LLC, Jersey City, New Jersey 07305.

18. Also on July 23, 2021, someone transferred $300,000 from PNC account ending 0378 to a Signature Bank account number of 6223 belonging to Prime Trust LLC. Prime Trust is a financial technology (fintech) company that acts as an intermediary between banks and cryptocurrency exchanges.

19. On July 26, 2021 another $183,620.00 was sent from Citizens Bank ending 8639 to PNC account ending 0378. This time, the beneficiary information listed was DDS Majestic LLC, Jersey City, New Jersey 07305.

20. Also on July 26, 2021, someone transferred $210,000 from PNC account ending 0378 to the Signature Bank account ending 6223 belonging to Prime Trust.

21. The total of the two transfers from Citizens Bank ending 8639 to PNC account ending 0378 was $513,720.00. The total of the two transfers from PNC account ending 0378 to Signature Bank account ending 6223 was $510,000.00

22. PNC account ending 0378 was opened in May 2021 and PNC Bank advised law enforcement that there was minimal activity in the account. The account was opened by Wayne Jackson, DOB 1989. Mr. Jackson's occupation was listed as firefighter and the account was set up for a home-based transportation service business.

23. A subpoena was issued to Prime Trust LLC regarding the receipt of the above two transactions totaling $510,000.00. A $300,000 wire was made on July 23, 2021, and a $210,000 wire was made on July 26, 2021. Prime Trust advised both wires were posted to Prime Trust account 940, which is held by BAM Trading Services Inc. (BinanceUS). BinanceUS is a cryptocurrency exchange where users can buy sell and/or trade cryptocurrencies.

24. A subpoena was issued to BAM Trading Services Inc. d/b/a BinanceUS regarding the two wires. The results showed that the funds were deposited into a BinanceUS account that was created on January 8, 2021 under the name Darren Stauffer, address of Kalamazoo, Michigan 49001, with an email address of dslogs717@gmail.com. The user ID on the BinanceUS account is 52374977. BinanceUS records confirm that a fiat deposit of $300,000.00 was made into Stauffer's account on July 23, 2021, and an additional fiat deposit of $210,000.00 was made into Stauffer's account on July 26, 2021. Those funds were eventually converted to cryptocurrency.

25. BinanceUS also provided email correspondence from the account creation process where BinanceUS requested additional documentation to set up Stauffer's account. That correspondence was with the ddslogs717@gmail.com email address. A driver's license was used

to set up the account, but the license was fraudulent. The photograph on depicted on the license is not of the true Darren Stauffer.

26. In summary, the above facts show that the BinanceUS account of Darren Stauffer with a User ID of 977 received $510,000.00 of victim funds. That account was fraudulently created using the email account ddslogs717@gmail.com.

BACKGROUND CONCERNING GOOGLE[1]

27. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

28. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

29. Signing up for a Google Account automatically generates an email address at the

[1] The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the "Google legal policy and products" page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

domain gmail.com. That email address will be the log-in username for access to the Google Account.

30. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services.

31. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

32. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

33. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

34. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

35. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

36. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

37. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Thus, stored

communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

38. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information and email (and the data associated with the foregoing, such as geo-location, date, and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

39. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

40. Other information connected to the use of a Google account may lead to the discovery of additional evidence. For example, the apps downloaded from the Google Play store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

41. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

42. Based on the forgoing, I request that the Court issue the proposed search warrant.

43. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

44. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

/s/ George Jasek
George Jasek
Special Agent
United States Secret Service

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Oct 14, 2021
Time: 8:38 AM, Oct 14, 2021

HONORABLE ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with ddslogs717@gmail.com ("the Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from January 1, 2021 through July 31, 2021, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);

2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);

3. Telephone numbers, including SMS recovery and alternate sign-in numbers;

4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery

numbers, Google Voice numbers, and alternate sign-in numbers

6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs;

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails; and

e. All forwarding or fetching accounts relating to the accounts;

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1343, Wire Fraud, those violations involving the user(s) of the account listed in Attachment A, occurring after January 8, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a) Records, information, and communications, in any form, which relate to a conspiracy to commit wire fraud;

b) Records, information, and communications, in any form, which relate to schemes to commit wire fraud;

c) Records, information, and communications, in any form, which relate to the identification of individuals who were victims of the schemes;

d) Records, information, and communications, in any form, which relate to the identification of individuals in order to secure their assistance in transferring stolen funds;

e) Records, information, and communications, in any form, which relate to incoming wire transfers and outgoing wire transfers of stolen funds;

f) Records, information, and communications, in any form, which relate to identification of bank accounts, cryptocurrency account, and brokerage accounts which contained unlawfully obtained funds;

g) The identity of the person(s) who communicated with the email accounts about matters relating to a wire fraud scheme or conspiracy or money laundering conspiracy, bank accounts, bank deposits, bank withdrawals, wire transfers, the purchase of prepaid debit cards, money orders, cashier's checks, cryptocurrency, and commissions, and the communications between those person(s), including records that help reveal their whereabouts;

h) Records, information, and communications, in any form, which relate to the personal or business relationships between participants in the offenses;

i) Communications, in any form, between the participants in the offenses;

j) Records, information, and communications, in any form, which relate to the identity or location (historic or current) of participants, co-conspirators, or aiders and abettors of the offenses;

k) Records, information, and communications, in any form, which relate to the identity of location of criminally-derived property;

l) Records, information, and communications, in any form, concerning financial accounts and transactions related to the items listed above;

m) Any records pertaining to the means and source of payment for services

(including any credit card or bank account number or digital money transfer account information or cryptocurrency account information);

n) Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

o) Evidence indicating the Account owner's state of mind as it relates to the crime under investigation; and

p) The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature